NIPPER STUDIO

Remotely auditing Check Point devices with Nipper Studio

Purpose: To explain how to audit a Check Point device using Nipper Studio remotely;

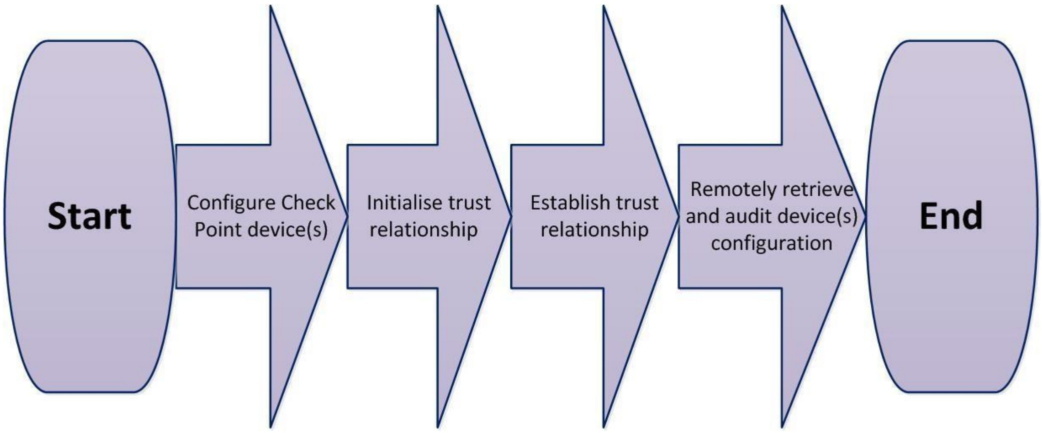
Scope: This method will work with all Check Point devices and with a Check Point management system. We describe how to set up your device using Check Point SmartDashboard, which is the recommended method. At the time of writing, this functionality is supported in Nipper Studio for Windows and CentOS, with further Linux distributions receiving support shortly. Mac is not presently supported;

<u>Additional Software required - </u> Check Point SmartDashboard - **https://www.checkpoint.com/**

Related documents: Nipper Studio Beginner's Guide, Nipper Studio CLI, and Nipper Studio help documentation.

Version: 1.0

Contents



Start
Configure Check Point device(s)
Initialise trust relationship
Establish trust relationship
Remotely retrieve and audit device(s) configuration
End

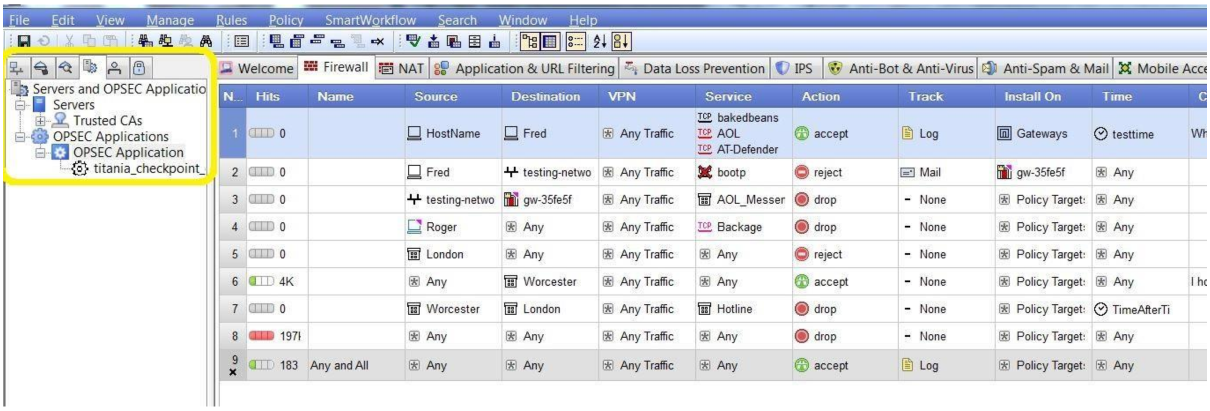
Configure your Check Point device(s)

Before you can retrieve the Check Point device configuration, you will need to make some changes to your Check Point device in order to allow Nipper Studio to connect to it.

You will need to have Check Point SmartDashboard installed on your workstation.

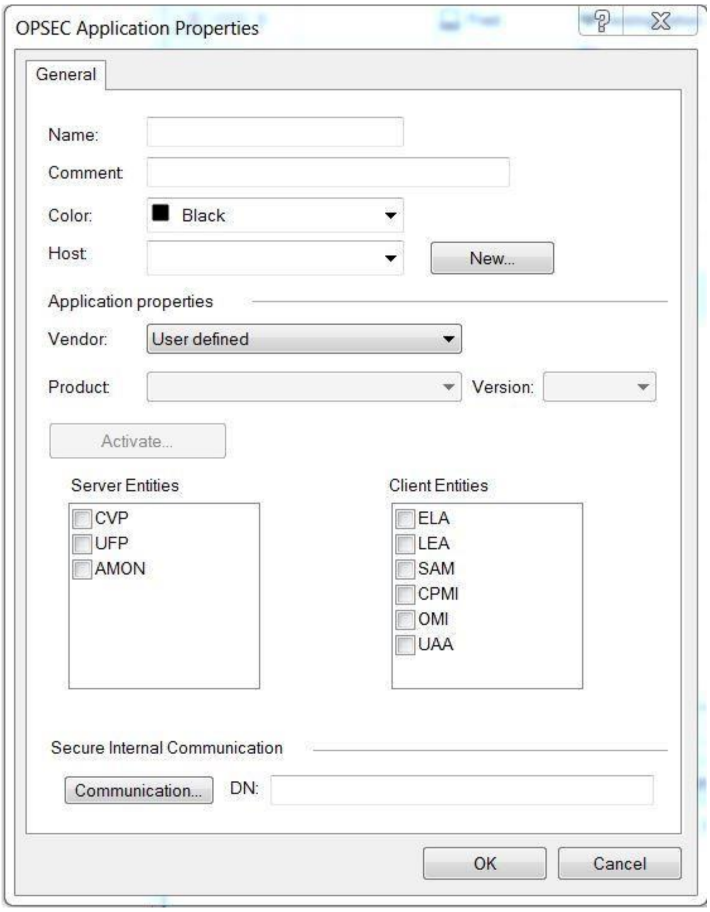
Log in to the device (or Management System) that you want to audit using Check Point SmartDashboard and then click the Firewall tab.

On the left hand pane of SmartDashboard select the Servers and OPSEC Applications tab – see below.



N...	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	C
1	0		HostName	Fred	Any Traffic	bakedbeans AOL AT-Defender	accept	Log	Gateways	testtime	Wh
2	0		Fred	testing-netwo	Any Traffic	bootp	reject	Mail	gw-35fe5f	Any	
3	0		testing-netwo	gw-35fe5f	Any Traffic	AOL_Messer	drop	None	Policy Target:	Any	
4	0		Roger	Any	Any Traffic	Backage	drop	None	Policy Target:	Any	
5	0		London	Any	Any Traffic	Any	reject	None	Policy Target:	Any	
6	4K		Any	Worcester	Any Traffic	Any	accept	None	Policy Target:	Any	I hc
7	0		Worcester	London	Any Traffic	Hotline	drop	None	Policy Target:	TimeAfterTi	
8	197I		Any	Any	Any Traffic	Any	drop	None	Policy Target:	Any	
9 ×	183	Any and All	Any	Any	Any Traffic	Any	accept	Log	Policy Target:	Any	

Right-click on OPSEC Applications then select New > OPSEC Application… Doing so will display the following OPSEC Application Properties screen.



OPSEC Application Properties

General

Name:

Comment:

Color: Black

Host:

Application properties

Vendor: User defined

Product:

Version:

Server Entities

☐ CVP
☐ UFP
☐ AMON

Client Entities

☐ ELA
☐ LEA
☐ SAM
☐ CPMI
☐ OMI
☐ UAA

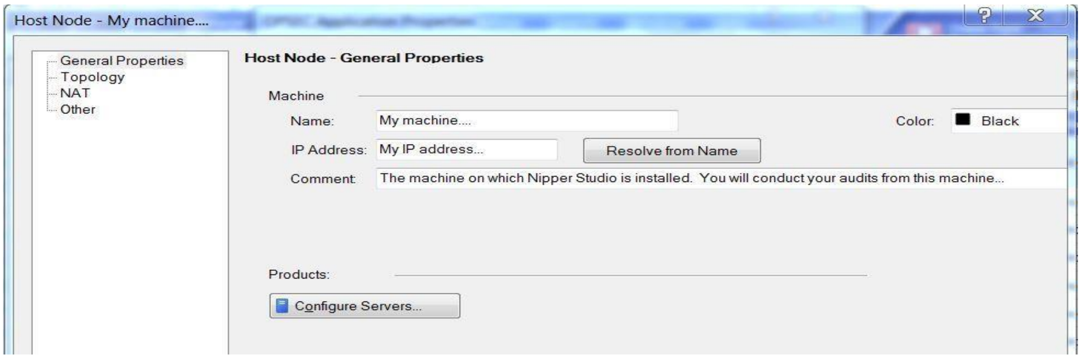
Secure Internal Communication

DN:

‘Name’ can be whatever you choose. We used ‘Nipper_Studio’ (note the lack of space; object names cannot contain spaces).

Add a ‘Comment’ if you wish – this may make it easier while auditing as the OPSEC application just creates an object on the firewall.

The ‘Host’ needs to have the IP address of the machine you are using for your Nipper Studio audits which has Nipper Studio installed on it. If you have already defined such a host, it will appear in the drop down menu, otherwise you will need to create a new one now using the ‘New…’ button, which will bring up the following screen:



Host Node - My machine....

Host Node - General Properties

Machine

Name: My machine....

Color: ■ Black

IP Address: My IP address...

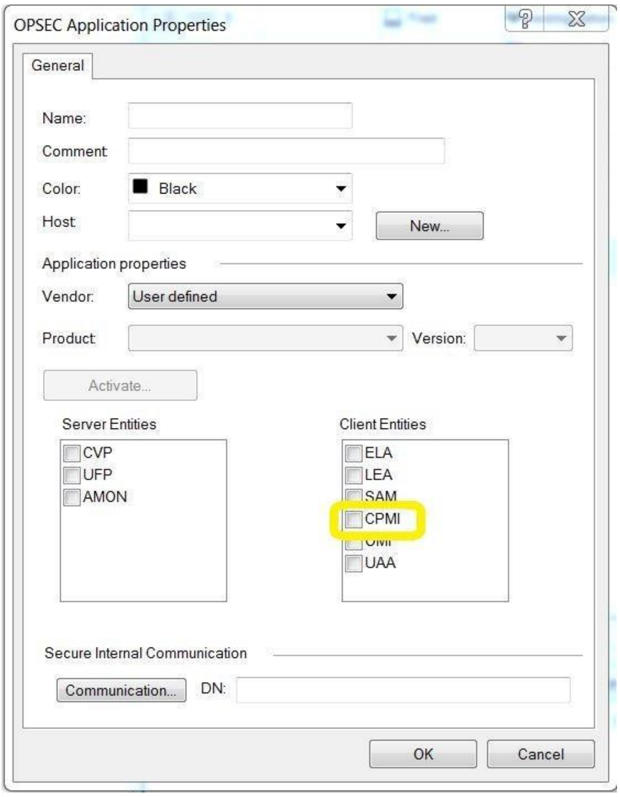
Comment: The machine on which Nipper Studio is installed. You will conduct your audits from this machine...

Products:

Enter the relevant details as indicated.
Returning to the OPSEC Application Properties dialogue box, you will now have details for ‘Name’, ‘Host’ and optionally ‘Comment’ and ‘Color’.

‘Vendor’ should be left as User defined.

In ‘Client Entities’ Check ‘CPMI’, do not select ‘OK’ yet.



OPSEC Application Properties

General

Name:

Comment:

Color: ■ Black

Host:

Application properties

Vendor: User defined

Product:

Version:

Server Entities

□ CVP
□ UFP
□ AMON

Client Entities

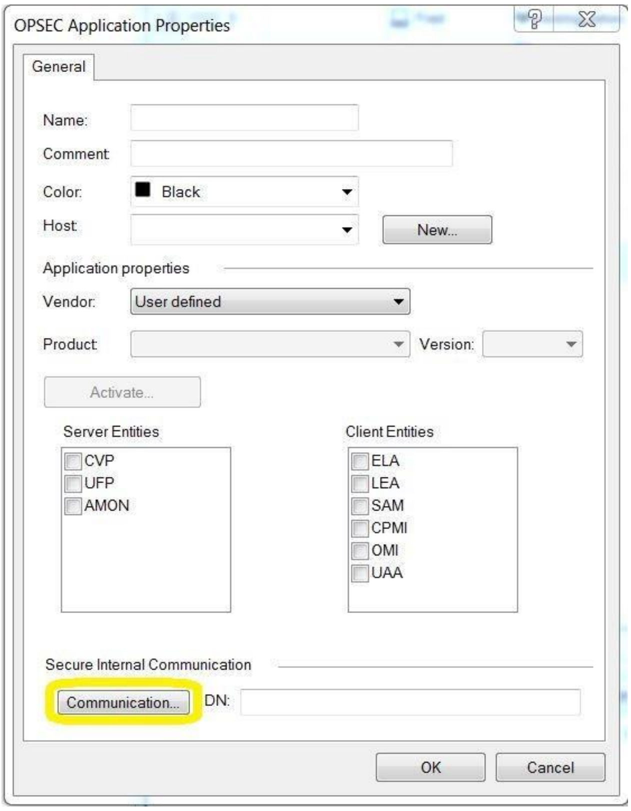
□ ELA
□ LEA
□ SAM
□ CPMI
□ OMI
□ UAA

Secure Internal Communication

DN:

Initialise trust relationship

Click on the ‘Communication’ button, as below:



OPSEC Application Properties

General

Name:

Comment:

Color: ■ Black

Host:

Application properties

Vendor: User defined

Product:

Version:

Server Entities

□ CVP
□ UFP
□ AMON

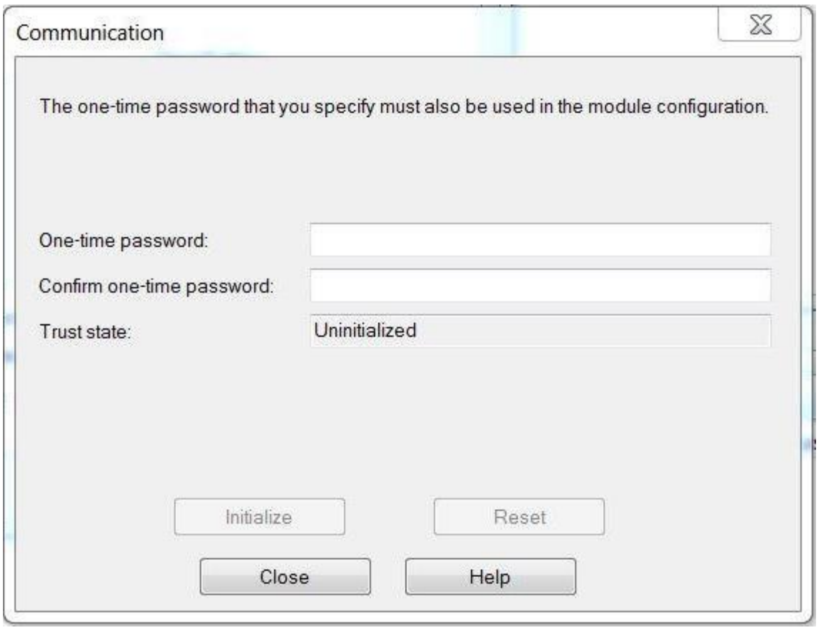
Client Entities

□ ELA
□ LEA
□ SAM
□ CPMI
□ OMI
□ UAA

Secure Internal Communication

DN:

This will bring up the following dialogue:



Communication

The one-time password that you specify must also be used in the module configuration.

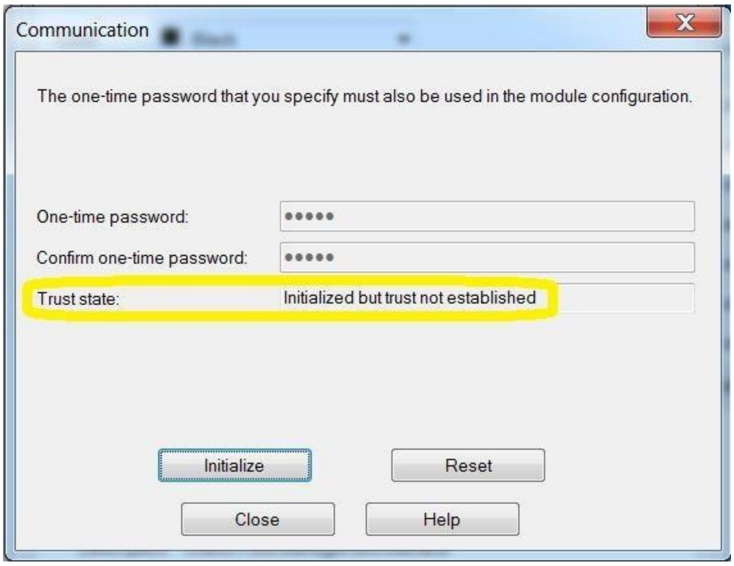
One-time password:

Confirm one-time password:

Trust state: Uninitialized

What we are doing here is creating the certificate used to authenticate the trust relationship. Enter and confirm the One-time password – **you will need to remember this password**.

Once you have done this, press the ‘Initialize’ button. You will see the ‘Trust state’ changed to ‘Initialized, but trust not established’, as below:



Communication

The one-time password that you specify must also be used in the module configuration.

One-time password: •••••

Confirm one-time password: •••••

Trust state: Initialized but trust not established

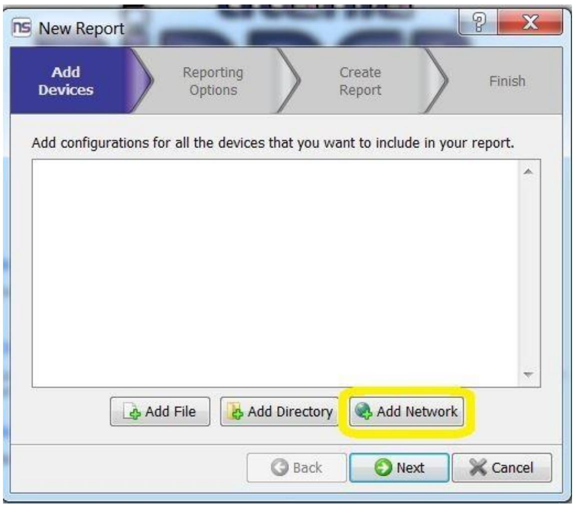
You can now close this dialogue, then click ‘OK’ on the OPSEC Application Properties screen **save the changes you have made by clicking the disk icon on the SmartDashboard toolbar.**

You have now completed the work you need to do on your Check Point device. The new OPSEC Application object will be visible in the left hand pane.

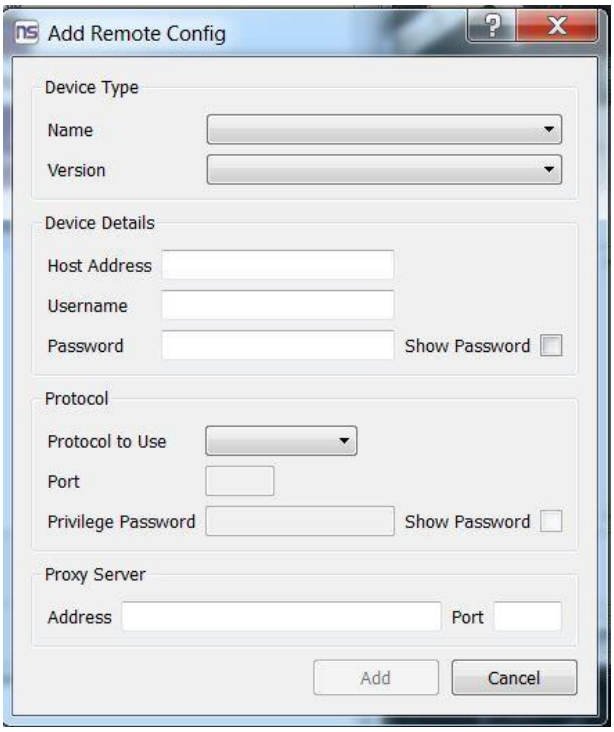
Establish trust relationship

Return to your Nipper Studio computer and run Nipper Studio.

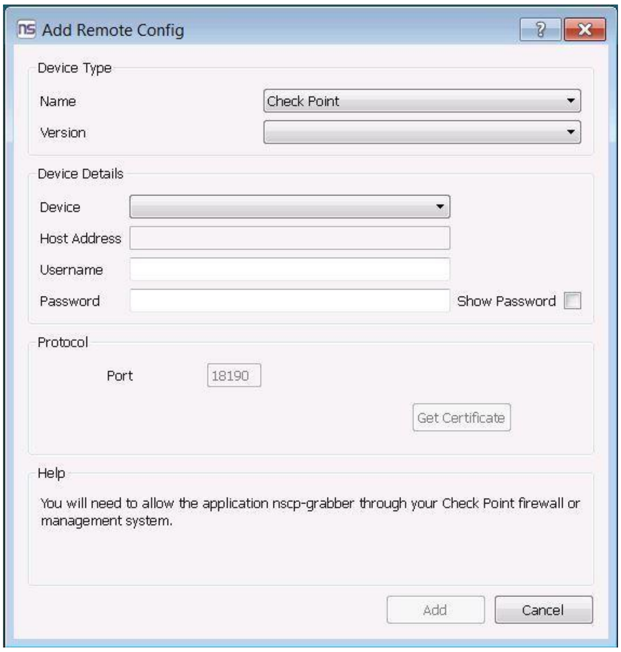
Go to 'New Report', and from the New Report dialogue, select 'Add Network':



This will bring up the following 'Add Remote Config' window:



From the ‘Name’ dropdown box, select ‘Check Point’. This will alter the ‘Add Remote Config’ window as follows:



Add Remote Config

Device Type

Name: Check Point

Version:

Device Details

Device:

Host Address:

Username:

Password:

Show Password □

Protocol

Port: 18190

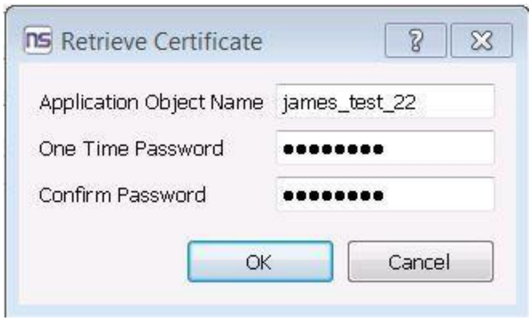
Help

You will need to allow the application nscp-grabber through your Check Point firewall or management system.

On the ‘Device’ drop down box, select ‘New…’ (Successfully added devices will appear here when you return to this screen later).

Add the Host Address of the Check Point device and its Username and Password.

Then click on ‘Get Certificate’. You will be prompted to enter the Application Object Name and your One-Time Password, as set above.



Retrieve Certificate

Application Object Name: james_test_22

One Time Password: ●●●●●●●●●

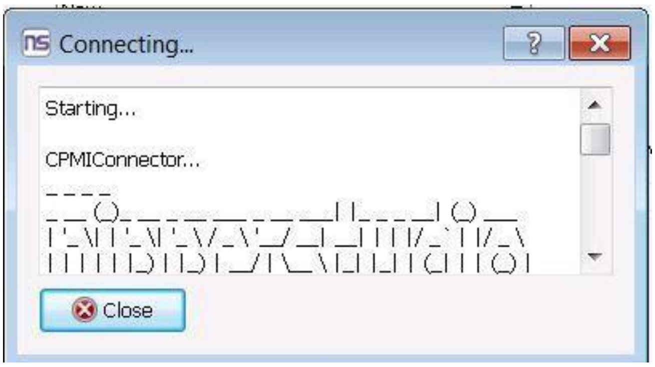
Confirm Password: ●●●●●●●●●

This will establish the trust relationship. This need only be done once per host machine.

Remotely retrieve and audit device(s) configuration

Leave the port as default and click ‘Add’.

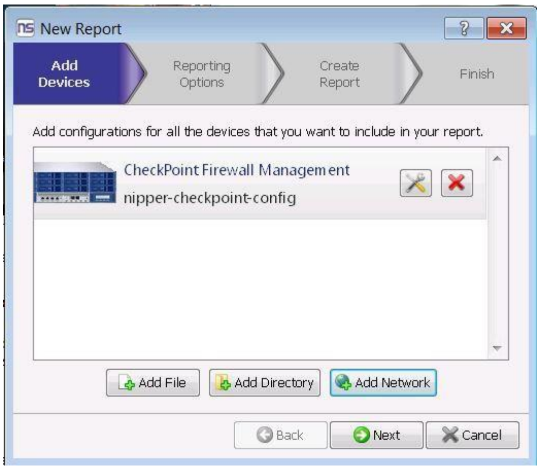
The following progress dialogue will be displayed:



```
Starting...

CPMIConnector...
```

Once complete the success message will be configuration will be imported as follows:



Add configurations for all the devices that you want to include in your report.

CheckPoint Firewall Management
nipper-checkpoint-config

Your Check Point configuration will be imported into Nipper Studio and the audit will begin.

Check Point configuration retrieval via the CLI

Please also see the Nipper Studio CLI guide, if required.

You can also use the CLI to establish the trust relationship and to connect and get you Check Point Firewall configuration.

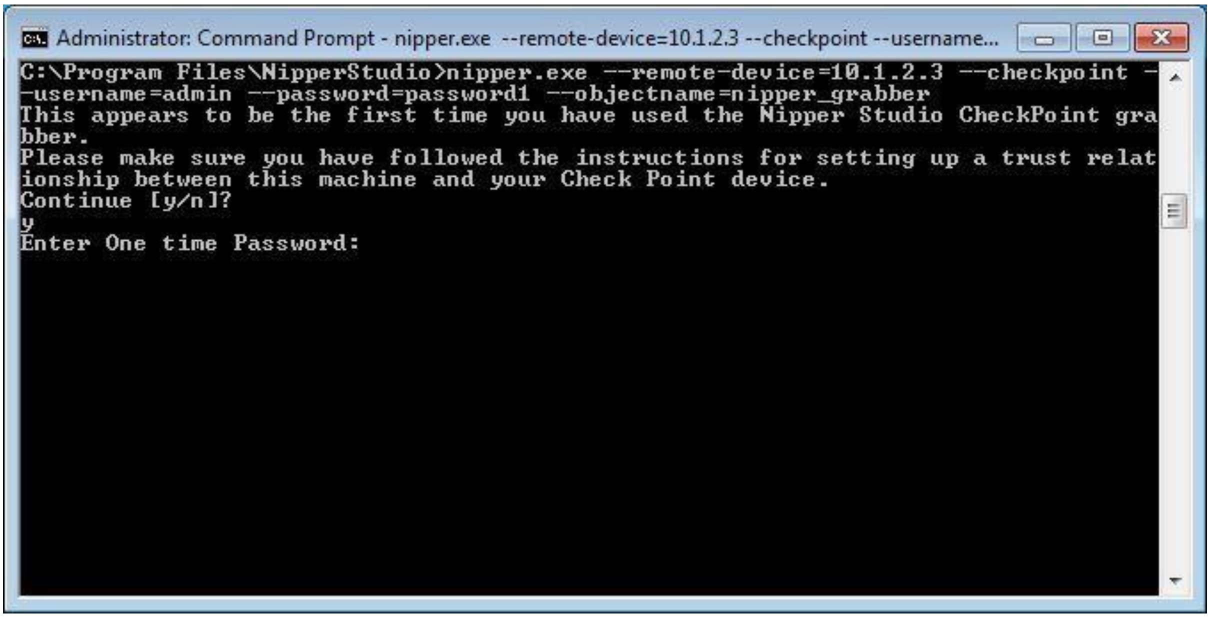
To do so, you can specify a remote device by using the --remote-device parameter, which takes the IP address of you Check Point firewall as the argument.

You will then need to add the following options, --checkpoint, which specifies this is a remote Check Point device, --username, which is the administrative username for the device, --password, which is the corresponding password, and finally --objectname, which is the name of the object that you specified when setting up the Check Point Firewall.

If you have yet to get the certificate from the device you will be prompted to continue, and then to enter the one-time password, otherwise Nipper Studio will carry on and retrieve the configuration.

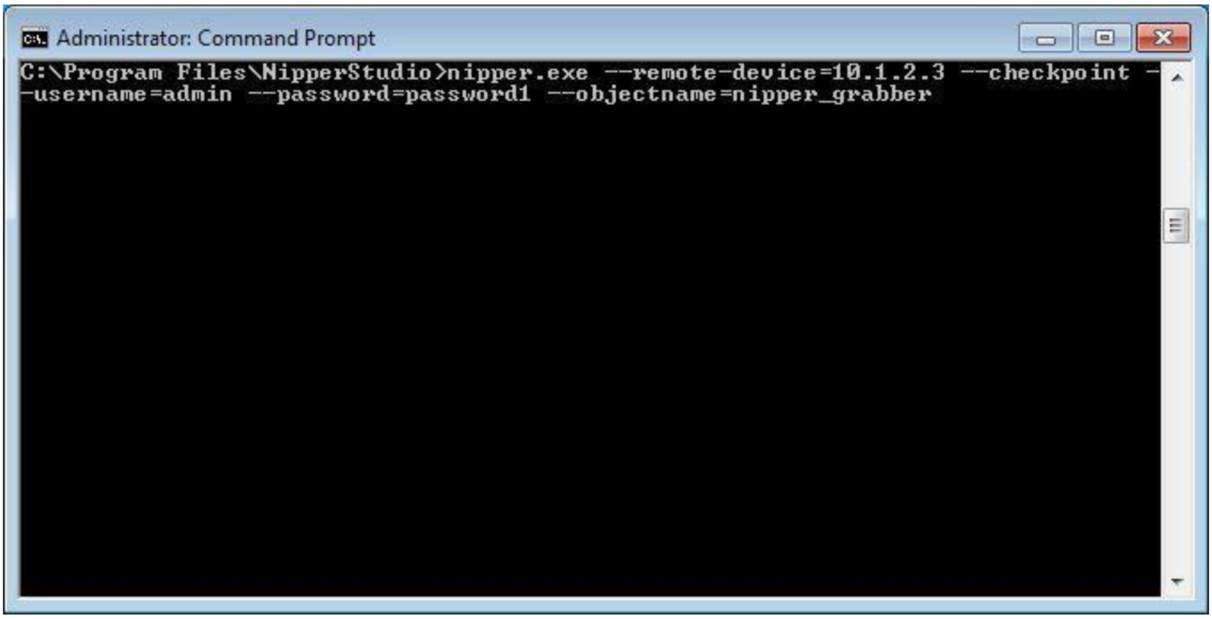
You can add additional arguments to the command line, just like normal, and Nipper Studio will process them, the Check Point device (assuming the configuration was retrieved successfully) will be treated like any other device that might have been specified.

The below images demonstrate using the command line on Windows. For Linux, the commands and options are the same



Administrator: Command Prompt - nipper.exe --remote-device=10.1.2.3 --checkpoint --username...

```
C:\Program Files\NipperStudio>nipper.exe --remote-device=10.1.2.3 --checkpoint -
-username=admin --password=password1 --objectname=nipper_grabber
This appears to be the first time you have used the Nipper Studio CheckPoint gra
bber.
Please make sure you have followed the instructions for setting up a trust relat
ionship between this machine and your Check Point device.
Continue [y/n]?
y
Enter One time Password:
```



```
C:\Program Files\NipperStudio>nipper.exe --remote-device=10.1.2.3 --checkpoint -
-username=admin --password=password1 --objectname=nipper_grabber
```

End of document.